



Capacity building workshop on cybercrime and electronic evidence
Colombo, Sri Lanka, 4-5 October 2013

The Budapest Convention on Cybercrime:

A framework for an effective international
criminal justice response to cybercrime

alexander.seger@coe.int

www.coe.int/cybercrime

1

About cybercrime prevention and criminal justice

Cybercrime

- ⇒ Offences against computer data and systems
- ⇒ Offences by means of computers
- ⇒ [electronic evidence in relation to any crime

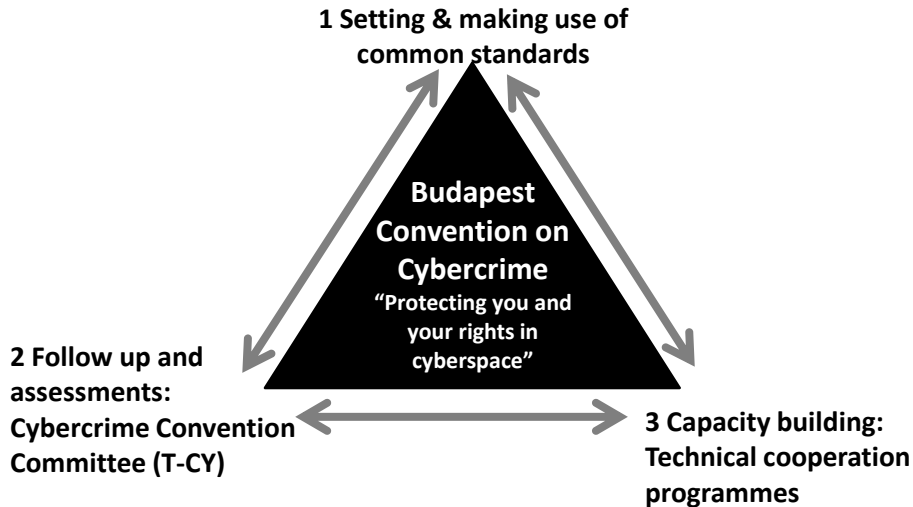
requires
⇒

Criminal justice response

- ⇒ Domestic substantive law
- ⇒ Domestic procedural powers (and safeguards)
- ⇒ Sufficient harmonisation to permit international cooperation
- ⇒ Specialised institutions
- ⇒ Law enforcement and judicial training
- ⇒ Interagency cooperation
- ⇒ Public/private cooperation
- ⇒ Efficient international cooperation
- ⇒ Link to cybersecurity agenda
- ⇒ Political commitment

2

The Budapest Convention as a framework



www.coe.int/cybercrime

3

Reach of the Budapest Convention

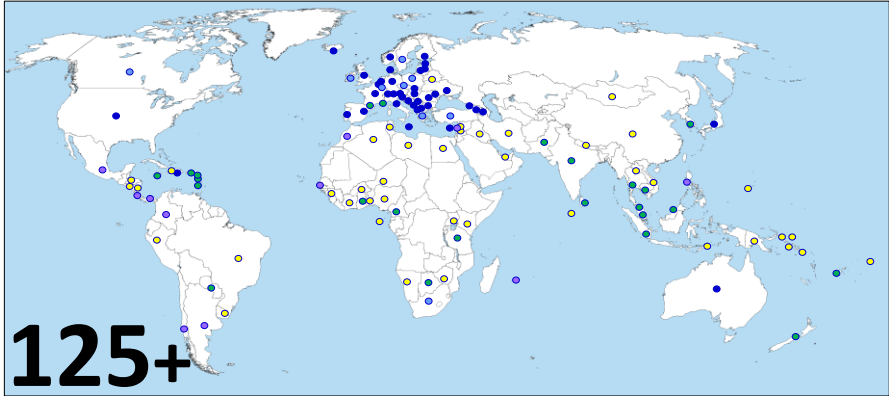
Opened for signature November 2001 in Budapest

As at May 2013:

- 40 parties (36 European, Australia, Dominican Republic, Japan and USA)
- 11 signatories (European, Canada, South Africa)
- 11 States invited to accede (Argentina, Chile, Colombia, Costa Rica, Israel, Mauritius, Mexico, Panama, Philippines, Senegal)
- = 62 States are parties/are committed to become parties/participate in Cybercrime Convention Committee at present
- Additional invitations to accede are in process
- Many more have used Budapest Convention as a guideline for domestic legislation

4

Reach of Budapest Convention

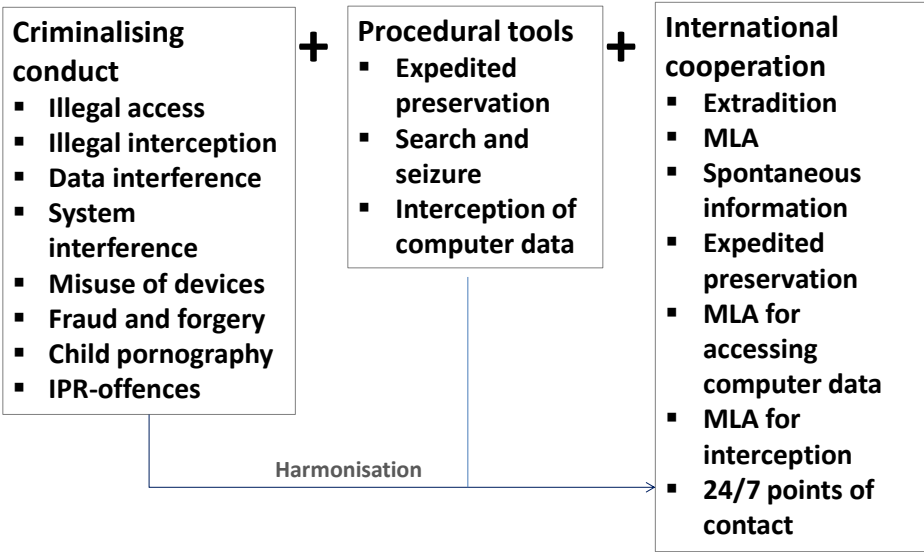


Indicative map only

- Ratified/acceded: 40 ●
- Signed: 11 ●
- Invited to accede: 11 ● = 62
- Other States with laws/draft laws largely in line with Budapest Convention = 20 ●
- Further States drawing on Budapest Convention for legislation = 43+ ●

5

Contents of the Budapest Convention



6

Budapest Convention: Asia/Pacific legislation

Examples:

- | | | |
|-----------------------------------|---|------------|
| ⇒ Australia (Party) | Council of Europe
cooperation on
legislation also with: | |
| ⇒ Brunei Darussalam | | |
| ⇒ Indonesia | | |
| ⇒ India | | |
| ⇒ Japan (Party) | | ⇒ Cambodia |
| ⇒ Korea | | ⇒ Laos |
| ⇒ Malaysia | | ⇒ Mongolia |
| ⇒ Pakistan | | ⇒ Vietnam |
| ⇒ Philippines (invited to accede) | | |
| ⇒ Singapore | | |
| ⇒ Sri Lanka | | |
| ⇒ Thailand | | |
| ⇒ Tonga | | |

7

About joining the Budapest Convention

THE COMMONWEALTH WORKING GROUP OF EXPERTS ON CYBERCRIME

REPORT TO COMMONWEALTH LAW MINISTERS 2014

“At the Commonwealth Law Ministers’ Meeting held in Sydney from 11 to 14 July 2011, Law Ministers ... mandated the Commonwealth Secretariat to form a multidisciplinary working group of experts to:

(ii) identify the most effective means of international co-operation and enforcement, taking into account, amongst others, the Council of Europe Convention on Cybercrime”

“... based on its content and accessibility, the criteria set out in paragraph 2.10 of this report, the Budapest Convention appeared to the Group to be currently the most effective and viable model for Commonwealth member states.”

“The Group recommends that Commonwealth countries should be encouraged

(i) to accede, where practicable, to the Budapest Convention; “”

8

About joining the Budapest Convention

Treaty open for accession by any State (article 37)

Phase 1:

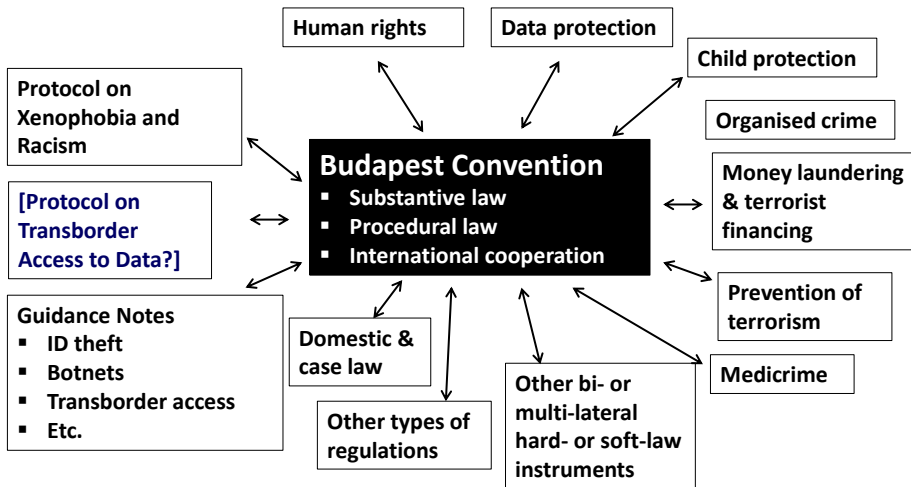
- If a country has legislation in place or advanced stage: Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
 - Deposit the instrument of accession at the Council of Europe
- ▶ **Acceded:** Australia, Dominican Republic
- ▶ **Invited:** Argentina, Chile, Colombia, Costa Rica, Israel, Mauritius, Mexico, Morocco, Panama, Philippines, Senegal

9

1 Common standards



A web of legal responses An even larger web of other responses

10

2

Follow up and assessments**Cybercrime Convention Committee (T-CY) – Article 46****Membership (status May 2013):**

- 40 Members (State Parties)
- 22 Observer States
- 10 International organisations (African Union Commission, ENISA, European Union, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Activities (examples):

- Assessment in 2012 of expedited preservation provisions (Articles 16, 17, 29 and 30)
- Assessment in 2013 of efficiency of international cooperation (Article 31 etc.)
- Guidance Notes (“botnets”, “spam”, “ID-fraud” etc.)
- Transborder access to data (Analysis of Article 32)
- Functioning of network of 24/7 contact points

www.coe.int/cybercrime

11

3

Capacity building**Capacity building: Technical cooperation programmes****Focus on:**

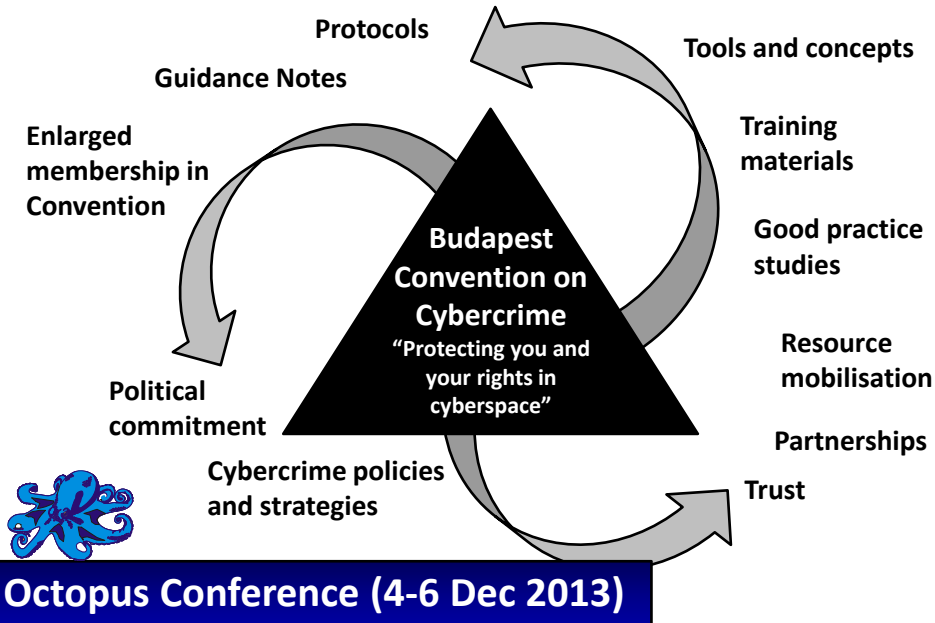
- Cybercrime strategies
- Legislation and safeguards
- Cybercrime units
- Law enforcement training
- Judicial training
- Financial investigations
- Protecting children
- Public/private cooperation
- International cooperation

Council of Europe global and regional projects:

- ▶ 500+ activities with 125+ countries & 130+ organisations and private sector since 2006
- ▶ New joint EU/COE project on **Global Action on Cybercrime in 2013**
- ▶ Encouraging other donors to provide assistance to countries in implementing Budapest Convention

12

A dynamic framework



13

Effectiveness/Impact of the Budapest Convention

- Stronger and more harmonised legislation
 - More efficient international cooperation between Parties
 - Better cybersecurity performance
 - More investigation, prosecution and adjudication of cybercrime and e-evidence cases
 - Trusted partnerships and public/private cooperation
 - Catalyst for capacity building
 - Contribution to human rights/rule of law in cyberspace
- = "Protecting you and your rights"

The Budapest Convention is in place and functioning.

Obstacles:

1. Limited criminal justice capacities
2. Political disagreements

www.coe.int/cybercrime

14

Benefits for Asia & Pacific region

Benefits

- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Technical assistance and capacity building

“Cost”: Commitment to cooperate

Disadvantages?

15

Contact for follow up

Alexander.seger@coe.int

Secretary of the Cybercrime
Convention Committee (T-CY)
Council of Europe
Strasbourg, France

www.coe.int/cybercrime

16